CONTINUATION OF APPLICATION FOR A SEARCH WARRANT AND IN SUPPORT OF A CRIMINAL COMPLAINT

INTRODUCTION

1. I, Aaron Eastham, am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed since 2018. I am currently assigned to the Detroit Field Office, Grand Rapids Resident Agency. During my employment with the FBI, I have conducted investigations involving violations of federal criminal laws, including violations related to child exploitation and pornography. I am familiar with the various statutes of Title 18, United States Code, Chapter 110 – sexual exploitation and other abuse of children, including violations pertaining to sexual exploitation and attempted sexual exploitation of children (18 U.S.C. § 2251(a)), distribution or receipt of child pornography (18 U.S.C. § 2252A(a)(2)), and possession of child pornography (18 U.S.C. § 2252A(a)(5)(B)). I am a federal law enforcement officer and, therefore, authorized by the Attorney General to request a Search Warrant under Federal Rule of Criminal Procedure 41.

2. Pursuant to the provisions of 18 U.S.C. § 2256(8), "child pornography" means a visual depiction, the production of which involves the use of a minor engaging in sexually explicit conduct, including but not limited to various simulated or actual sex acts, or the lascivious exhibition of the genitals or the pubic area.

3. Based on the information set forth below, there is probable cause to believe that evidence of violations of federal law, specifically, of coercion and enticement of a minor (contrary to 18 U.S.C. § 2422(b)), sexual exploitation and attempted sexual exploitation of a child (contrary to 18 U.S.C. § 2251(a)), receipt of

child pornography (contrary to 18 U.S.C. § 2252A(a)(2)), and possession of child pornography (contrary to 18 U.S.C. § 2252A(5)(B)), will be found on ANDREW SORENSEN's Apple iPhone (hereinafter the "SUBJECT DEVICE"), described more fully in Attachment A. The categories of electronically stored information and evidence sought are described in Attachment B. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

4. The statements contained in this Continuation are based upon information acquired during my investigation, as well as information provided by others such as other police officers, task force officers (TFOs), and special agents of the FBI. Because this Continuation is being submitted for the limited purposes described above, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause.

PROBABLE CAUSE FOR SEARCH WARRANT

5. Discord is an online voice, video, and text chat application. On 1/24/2023, an administrator of an online Discord server submitted an online tip to the FBI's National Threat Operations Center, regarding Discord User Guitar_Concept#3687, who the Tipster identified as ANDREW SORENSEN, but who went by the name "Andrea." According to the Tipster, SORENSEN was in an inappropriate online relationship with a 13-year-old transgender minor.

6. On 2/28/2023, the Tipster was telephonically interviewed by law

enforcement. The Tipster ran an LGBTQ mental health support group server on Discord for minors. SORENSEN was also an administrator in this group. A 13-year-old Discord user named Colby_Brock#8176 (later identified as a 13-year-old biological female,[1] who went by the name Colby and identified as a male, herein referred to as MV1) told the Tipster that she was in a relationship with Guitar_Concept#3687. The Tipster removed SORENSEN from the group after several other minors reported him for inappropriate behavior.

7. The Tipster identified SORENSEN's Facebook profile and sent a screenshot of the profile to the FBI. The profile was under the name "Andrew Sorensen III". An Agent from FBI viewed SORENSEN's public-facing Facebook profile. The profile contained several selfie-style photos that were used for profile pictures for the account. It also contained a link the user's Twitch profile,[2] which was under the name "Guitar_Concept." In the profile's "About Info," the current city was listed as Muskegon, Michigan and the user's birthday was 12/ XX/2000.[3]

8. The Tipster identified MV1 as living in Palatine, Illinois and had made a report with the Palatine Police Department regarding SORENSEN's relationship with MV1. Law Enforcement spoke with MV1's mother, who said the MV1 was in an out-patient hospitalization program. MV1's mother knew MV1 had been in an online

[1] Her name is known to me; however, to protect personal information of the minor, I have not included it here.

[2] Twitch is an online, interactive livestreaming service for video and audio content.

[3] The full date of birth is known to me; however, I have not included it here to protect personal identifying information.

relationship with SORENSEN, but did not know SORENSEN's age or legal gender. She was also aware MV1 had sent SORENSEN "inappropriate" pictures in the past, but they have since been deleted. MV1's mother did not think SORENSEN asked for MV1 to meet in person or send inappropriate pictures. MV1's mother would not consent to MV1 being forensically interview by law enforcement at that time.

9. On 3/23/2023, the FBI served an administrative subpoena to Discord for the account Guitar_Concept#3687, requesting basic subscriber information for the account user. Discord provided the following subscriber information:

a. Phone Number: +12312151942

b. E-mail Address: tyandandrewsorensen@gmail.com

c. Last Seen IP: 71.227.108.195 on 2023-03-24.

10. The IP address 71.227.108.195 was analyzed using a free online GeoIP2 Web Service. The IP addressed resolved to Muskegon, Michigan.

11. A Michigan Secretary of State search was conducted for ANDREW SORENSEN. The birthday listed on SORENSEN's driver's license matched the date listed on the ANDREW SORENSEN III Facebook profile (12/XX/20000). The person in the driver's license photo also matched the person in the selfie-style photos observed on the ANDREW SORENSEN III Facebook page.

12. On Friday, 12/22/2023, law enforcement interviewed SORENSEN in-person at his home in Norton Shores, Michigan. Norton Shores is a municipality within Muskegon County. The interview was set up by law enforcement after they spoke with SORENSEN's grandmother and left a phone number for him to call.

SORENSON returned the call from telephone number 231-215-1942, which was the number associated with the Guitar_Concept#3687 Discord account. During the interview, SORENSEN said that his Discord username was "Guitar_Concept" and that Discord had gotten rid of the numbers at the end of the username.[4] SORENSEN said he was part of "mental health" group chats on Discord. He stated that he only used Discord on his phone and had his current phone for approximately 3 years.

13. SORENSEN admitted to talking with a Discord user named "Colby" about a year ago. He said he thought she might have been 14-years-old. SORENSEN admitted to sending MV1 two pictures of his penis and that she sent him three photos of her bare chest and two photos of her vagina. At first, SORENSEN denied asking MV1 for the photos and said that she just sent them to him, but then he admitted that he requested the nude photos from her.

14. At the end of the interview, law enforcement seized SORENSEN's phone to prevent the destruction of evidence, until a search warrant could be obtained. The U.S. Attorney's Office has informed me that an officer may seize personal property without a warrant if the officer has a reasonable suspicion that the property contains evidence of a crime. *See United States v. Avery*, 137 F.3d 343, 349 (6th Cir. 1997). Law enforcement seized the phone because they believed the cell phone contained evidence of child pornography, as outlined more fully herein. The phone was located on SORENSEN's person prior to it being seized. In my training and experience with

[4] Publicly available content on Discord's site regarding updates confirms that the company was moving away from more complicated usernames that contained various digits. *See* https://discord.com/blog/usernames.

child pornography investigations, had law enforcement left the cell phone with SORENSEN, any evidence related to the child pornography would have been likely and imminently destroyed. They seized the phone to prevent destruction of potential evidence. The phone, referred to as the SUBJECT DEVICE, is further described in Attachment A.

15. On 12/22/2023, law enforcement submitted a preservation request to Discord for the Guitar_Concept#3687 / Guitar_Concept account.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

16. Based on my training, experience, and information obtained from other agents, I know the below statements are accurate.

17. Computers and digital technology such as cell phones are the primary way in which individuals interested in child pornography interact with each other. Computers and digital technology such as cell phones basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

18. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as WiFi or Bluetooth. Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone.

These memory cards are often large enough to store thousands of high-resolution photographs or videos.

19. Any computer can connect to any smartphone, tablet, or other computer. Through the internet, electronic contact can be made to millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

20. The computer's or phone's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - computer hard drives, external hard drives, CDs, DVDs, and thumb, jump, or flash drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

21. The internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

22. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

23. Individuals commonly use smartphone and computer apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

24. Communications by way of computer or phone can be saved or stored on the device used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or device's user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

25. Based upon my knowledge, experience, and training in child exploitation and child pornography (CP) investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals with a sexual interest in children. These characteristics particularly apply to individuals involved in possessing or distributing CP online, including those accessing websites whose primary content is CP. These common characteristics include that the individuals:

a. Generally have a sexual interest in children and receive sexual gratification from viewing children engaged in sexual activity or in sexually suggestive poses, or from literature describing such activity.

b. May collect or view sexually explicit or suggestive materials, including child erotica, in a variety of media, including in hard copy and/or digital formats. CP viewers and collectors oftentimes use these materials for their own sexual arousal and gratification. They may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse or groom a child to participate in sexual activity, or to demonstrate desired sexual acts to a child. They may also use toys, games, costumes, sexual clothing, sexual paraphernalia, and children's clothing to lure or entice children. They may keep "trophies" or mementos of sexual encounters with children, or items that they use to gratify a sexual interest in children, such as by collecting children's

underwear or other items belonging to a child.

c. May take photographs that either constitute CP or indicate a sexual interest in children by using cameras, video cameras, web cameras, and cellular telephones. Such images and videos may be taken with or without the child's knowledge. This type of material may be used by the person to gratify a sexual interest in children.

d. Generally maintain their collections in a safe, secure, and private environment. These images and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media). The images can be stored in both digital and hard copy format and are usually hidden so that they are not found by other members of the residence or by anyone else who enters the home. Such hiding places could include but are not limited to garages, sheds, attics, vehicles, bags, and pockets. Digital files and devices may be password protected, encrypted, or otherwise protected.

e. Often maintain their collections of CP and other materials indicating a sexual interest in children for a long period of time—commonly over the course of several years. These collections are also frequently maintained despite

changes in residence or the acquisition of different or newer computer devices.

f. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other CP distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same interests in CP. Such correspondence may take place, for example, through online bulletin boards and forums, internet-based chat messaging, email, text message, video streaming, letters, telephone, and in person. In some cases, these individuals may have joint involvement in CP activities with others within their household or with whom they share a close relationship (e.g., brothers/siblings dating partners, or coworkers).

SPECIFICS OF SEIZING AND SEARCHING COMPUTER AND PHONE EVIDENCE

26. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

27. I know based on my knowledge, training, and experience that:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium or electronic device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in what is commonly referred to as a swap or recovery file;

b. Computer or phone files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;

c. Wholly apart from user-generated files, computer or phone storage media—in particular, internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer or phone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information; and

d. Files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or cache.

28. As further described in Attachment B, this application seeks permission to locate not only device files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes

how devices were used, the purpose of their use, who used them, and when. Probable cause exists that this forensic electronic evidence will be on the SUBJECT DEVICE.

29. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer or phone file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

30. Information stored within a computer, phone, and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer, phone, or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection

programs) can indicate who has used or controlled the computer, phone, or storage media.

31. This user attribution evidence is analogous to the search for indicia of occupancy while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer or phone owner. Further, computer, phone, and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers and phones typically contain information that logs user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the device, and the IP addresses through which the device accessed networks and the internet. Such information allows investigators to understand the chronological context of device access, use, and events relating to the crime under investigation.

32. Some information stored within a computer, phone, or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or phone may both show a particular location and have geolocation information incorporated into its file data. Such file data also typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and

timeline information described herein may either inculpate or exculpate the computer user.

33. Information stored within a computer or phone may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

34. A person with appropriate familiarity with how a computer or phone works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

35. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer and phone evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or phone is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

36. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

37. I know that when an individual uses a computer or phone to obtain or access child pornography, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer or phone used to commit a crime of this type may contain data that is evidence of how the device was used, data that was sent or received, notes as to how the criminal conduct was achieved, records of internet discussions about the crime, and other records that indicate the nature of the offense.

38. Computer and phone users can attempt to conceal data within equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension .jpg often are image files. A user can easily change the extension to .txt to conceal the image and make it appear that the file contains text. Computer and phone users can also attempt to conceal data by using encryption. Encryption

involves the use of a password or device, such as a dongle or keycard, to decrypt the data into readable form.

39. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit imaging, or otherwise copying the SUBJECT DEVICE and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium. This might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. Because the SUBJECT DEVICE is in the custody of the government, and it will obtain the records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

JURISDICTION

40. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See also* 18 U.S.C. § 2703(a), (b)(1)(A), (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

CONCLUSION

41. Based upon the above information, I respectfully submit there is probable cause to believe that on the SUBJECT DEVICE there will be evidence, fruits, and instrumentalities of the crimes of coercion and enticement (18 U.S.C. §§ 2422(b)), sexual exploitation and attempted sexual exploitation of a child (18

U.S.C. § 2251(a)), receipt of child pornography (18 U.S.C. § 2252A(a)(2)), and possession of child pornography (18 U.S.C. § 2252A(a)(5)(B)), the "subject offenses" that have been committed by ANDREW SORENSON.

42. Accordingly, I request that the Court issue the proposed search warrant, described in Attachment A for items listed in Attachment B.